MORAL SENSITIVITY IN INFORMATION SECURITY DILEMMAS

Research in Progress

Mohammadnazar, Hojat, University of Jyväskylä, Jyväskylä, Finland, homohamm@student.jyu.fi

Ghanbari, Hadi, University of Jyväskylä, Jyväskylä, Finland, hadi.ghanbari@jyu.fi

Siponen, Mikko, University of Jyväskylä, Jyväskylä, Finland, mikko.t.siponen@jyu.fi

Abstract

Activities that undermine information security such as noncompliance with information security policies raise moral concerns since they can expose valuable information assets. Existing research shows that moral reflection could play an inhibitory role in one's decision to undermine information security. However, it is not clear whether users interpret such decisions from a moral standpoint to engage in moral reflection in the first place. Users have to be morally sensitive before they engage in moral reflection. Moral sensitivity involves perceiving a situation as morally relevant, identifying the parties involved and perceiving possible courses of action. We examine moral sensitivity in security dilemmas in a Finnish university setting. We develop audio records of conversations about two policy compliance scenarios, each involving moral concerns. After playing back these audio records to participants, we pose probing questions to examine their moral sensitivity. Our preliminary results indicate that users may not be sensitive towards the moral concerns raised by security dilemmas. Based on our findings, we suggest providing users with information regarding those affected by security decisions, IT capabilities in an organization and the possible consequences of different courses of action in security education programs rather than directives about morally right or wrong behavior.

Keywords: Information security, Information security policy compliance, Moral sensitivity, Moral behavior

1 Introduction

Information security embodies a moral quality insofar as it regards protection of privacy and intellectual property. Activities such as noncompliance with information security policy and information system misuse could leave an organization vulnerable to threats from malicious insiders and outsiders. Such threats could lead to data breaches exposing valuable personal and organizational information assets. As such, activities that undermine information security raise moral concerns.

Having recognized such moral concerns, previous research has laid out the role of moral reflection in users' information security decisions. Given an inhibitory role, moral beliefs, judgments, obligations, and ideologies are shown to prevent users from engaging in policy noncompliance (Yazdanmehr & Wang 2016; Vance & Siponen 2012; Li et al. 2014), IT misuse (Banerjee et al. 1998; Kim et al. 2016; D'Arcy & Devaraj 2012), and various other activities that could undermine security (Hansen & Walden 2013). However, moral reflection presupposes the realization that one is facing a moral problem. Without such realization, one might not reflect on a situation in moral terms at all. In other words, in the absence of the realization that one is facing a moral problem, moral beliefs, judgments, obligations, and ideologies may become irrelevant to decision-making. This realization occurs in a process referred to as moral sensitivity (Rest 1982).

In information security research settings, researchers often presuppose or inadvertently trigger moral sensitivity. For instance, when asked whether information security policy violation is morally right, participants may not be able to perceive the moral relevance of security policy violation or may misinterpret the moral problem altogether. Researchers' analysis of participants' responses, in this case, however, presupposes that security policy violation as a moral problem has been understood and correctly interpreted. Alternatively, terms such as "morally right" in such a question might provide participants with cues indicating the presence of a moral problem, in turn, triggering their moral sensitivity. However, at workplace or at home, users are on their own to interpret the situation. Unfortunately, despite a few attempts (Goles et al. 2006; Dorantes et al. 2006), it is unclear whether users interpret activities that undermine information security in moral terms. This leaves the relevance of previous findings with regards to moral inhibition hanging in balance.

In this study, we examine users' moral sensitivity toward information security policy compliance by playing back pre-recorded audios of conversations between two colleagues. Each scenario includes a morally relevant security dilemma. These scenarios are password sharing and email security. According to Rest (1982), moral sensitivity involves perceiving a situation as morally relevant, identifying the parties involved and perceiving possible courses of action. Consequently, we ask participants to explain the problem in each incident, identify the parties involved and describe courses of action possible after listening to each pre-recorded audio. Listening to an audio record of a morally relevant situation does not tip off the participant to engage in moral reflection. This method is similar to the one deployed by Bebeau, Rest, and Yamoor (1985) and that of Volker (1984).

Our results would, first and foremost, indicate whether users are morally sensitive towards security policy noncompliance, in particular, password and email policies. Should organizational users be unaware of the moral relevance of security policies they may not engage in any form of moral reflection. Resultantly any security awareness and education program that suffices to provide users with directives about morally right or wrong behavior may fail to yield expected results. Our results highlight the necessity of accounting for moral sensitivity when the role of user's moral reflections in information security is studied. Further, in this research, we utilize a method that draws responses from participants without unintentionally tipping them off or without presupposing their understanding of moral concerns in security. This method paves the path for future research to investigate users' moral sensitivity toward various morally significant phenomena.

2 Background

Previous research has indicated that moral reflection could play an inhibitory role in users' decisions regarding noncompliance with information security policy and IT misuse. Such a role could be seen

when individuals' moral beliefs, their perceptions of moral acceptability and their idealistic and relativistic beliefs are investigated.

In this regard, one's belief in the moral wrongness of security policy violation has been reported to lower one's intention to violate the policy (Bansal et al. 2016; Vance & Siponen 2012; Tilahun & Tibebe 2017). Along the same lines, belief in moral inappropriateness of non-work-related internet usage has been linked to increased intention to comply with internet use policy (Li, Sarathy, et al. 2010; Li, Zhang, et al. 2010; Li et al. 2014). While these studies indicate that moral inhibition could lead to increased policy compliance, lack of moral inhibition has been linked to increased security policy violation. D'arcy et al. (2014) argued that users' moral disengagement in the face of stressful security requirements increased policy violation intention. It is important to note that moral disengagement as an emotion-based and cognitive coping mechanism (D'Arcy et al. 2014), presupposes that one has already been morally engaged. In other words, for one to morally disengage as a coping mechanism, first they have to be morally sensitive.

In corroboration with these findings, studies into IT misuse have also reported evidence of the inhibitory role of moral reflection on users' decision-making. One's belief in moral unacceptability of unauthorized access and modification of information, for instance, has been found to be linked to decreased intention to access or to modify information without authorization (D'arcy & Hovav 2009). Similarly, finding a misuse action morally unacceptable, has been reported to lower intention to misuse in multiple studies (D'Arcy & Devaraj 2012; Yoon 2011; Loch & Conger 1996; Cronan et al. 2005). This decrease in intention to misuse has been observed across different cultures (Hovav & D'Arcy 2012).

Inspection of idealistic and relativistic beliefs based on Forsyth's (1980) characterization of such beliefs has also revealed similar results. Forsyth (1980) proposed that idealism is the extent to which a desirable outcome can be achieved by doing the right thing. On the other hand, he defined relativism as the degree to which one believes universal and rigid moral rules determine right or wrong. The less one believes in universal moral rules, the more relativistic they are. Dorantes et al. (2006) argued that idealistic and relativistic beliefs could shape one's intentions to misuse IT indirectly by affecting their perception of a scenario's moral intensity. Additionally, Peterson (2002) found evidence that those who subscribe to the idea of universal moral rules (high idealists) intend less to misuse computers.

Despite previous research findings indicating an inhibitory role for moral reflection in information security decisions, one shall note that moral reflection can occur when a moral agent realizes they are facing a moral problem. In fact, well-known theories of moral decision-making such as the four-component model (Rest 1986), issue-contingent model (Jones 1991) and ethical decision-making theory (Hunt & Vitell 1986) all propose that an initial realization of a moral problem is essential to moral decision-making. The process by which one arrives at this initial realization is referred to as moral sensitivity (Rest 1982). Moral sensitivity as the first component of the four-component model (Rest 1986) refers to one's awareness of moral situations and the effect of actions on other people. Moral sensitivity involves perceiving a situation as morally relevant, identifying the parties involved, and perceiving possible courses of action and their consequences for those involved (Rest 1982). Moral sensitivity has been associated with empathy and role-taking abilities (Myyry & Helkama 2002) and it is suggested to consist of both cognitive and affective elements.

Except for a few studies (Goles et al. 2006; Dorantes et al. 2006), moral sensitivity seems to have been overlooked in previous information security research. Studies that have examined the role of moral reflection in users' information security decisions commonly instruct participants to engage in moral reflection. For instance, Vance and Siponen (2012) asked participants whether "It is morally right to violate company IT security policies". Answering this question requires the participant to perceive and understand the problem. This may not be the case. The participant might not perceive the moral relevance of security policy violation or may misinterpret the moral problem altogether. Alternatively, researchers' use of terms such as "moral", "ethical", "right" or "wrong" in their questionnaires might act as cues tipping off the participants that they face a morally relevant situation, in turn, triggering their moral sensitivity. Unfortunately, this problem persists even in studies in which moral sensitivity is specifically studied. Dorantes et al. (2006) and Goles et al. (2006), for instance, addressed moral

sensitivity by asking their participants whether a number of information technology misuse scenarios "involves an ethical problem". As much as such efforts deserve credit, they still fall short in determining whether users realize that IT misuse poses a moral problem. On the other hand, the very terms "an ethical problem" in the question might tip off the participants to reflect on the scenario in moral terms and as such does not capture whether participants are capable of realizing the presence of a moral problem on their own. The same shortcoming appears in a number of studies regarding unauthorized software copying (Chan et al. 2013; Moores & Chang 2006; Hansen & Walden 2013).

Overlooking moral sensitivity in the literature raises questions regarding the applicability of previous research findings. That is, if users are not able to interpret the moral problem in a situation, whether moral reflection plays an inhibitory role in their decision-making becomes irrelevant. Without understanding the moral problem in a situation, users might not engage in moral reflection at all. In fact, in the wake of a finding that contrasted the previously known 'higher is better' preference rating for levels of moral reasoning, Myyry et al. (2009) speculated that perhaps their participants did not view noncompliance with password security policy a moral issue at all. In such a situation, participants' responses may have been based on other considerations. In this research, therefore, we focus on users' moral sensitivity toward security policy noncompliance. Particularly, we strive to examine moral sensitivity without presupposing or inadvertently triggering moral sensitivity.

3 Method

We examined moral sensitivity toward security policy noncompliance without presupposing users' understanding of the moral relevance of compliance or inadvertently triggering their realization of a moral problem. To this end, we developed audio records of conversations between two colleagues based on two policy compliance scenarios, each involving moral concerns. The policy compliance scenarios dealt with (1) password sharing and (2) email security in a university setting. In the password sharing scenario a lecturer faces a dilemma in which she either has to share the password to her laptop with a secretary in order to submit student grades or find another solution. The email security scenario concerns a post-doctoral researcher who has received an email from an applicant for doctoral studies but suspects the origins of the email. Scenarios are presented in the appendix. We played back these audio records to participants and asked them probing questions to determine their sensitivity toward moral concerns in the scenarios. This method is similar to the one deployed by Bebeau, Rest, and Yamoor (1985) and that of Volker (1984) and has not been used in information security research before. Compared to other approaches to studying moral sensitivity such as surveys (Sparks 2015) and scenario methods, the approach taken in this study provides participants with contextual information and requires them to take the role of the protagonist in the scenario. This is particularly of value since moral sensitivity is known to be associated with one's role-taking abilities (Myyry & Helkama 2002). Listening to records of morally relevant situations would not tip off the participant to engage in moral reflection, since the records do not contain any indication of a moral problem. Furthermore, we do not instruct participants to engage in moral reflection by any means. In this manner, interpretation of the situation is left to the participants themselves.

3.1 Development of audio records

In order to develop the audio records, we first examined the security policy at the university in which we intended to carry out the research. Considering the policy, we created two scenarios of policy compliance regarding password sharing and email security. From these scenarios, we developed scripts of conversations between two colleagues. These scripts were read by voice actors (fluent in English) and recorded. None of the authors was involved in voice acting the conversations. This was done to make sure that participants would not associate characters in the audio records with the researchers.

Students and staff at the university were required to know and comply with the information security policy. Despite this, in order to make sure that participants were aware of the terms of the security policy and what counted as a violation (Siponen & Vance 2014), we included the relevant terms of the policy in each audio record. This was done by designing each audio record in two episodes. In the first episode

of each audio record, two colleagues discuss the policy and its importance. Moreover, considering the variation in the type of information accessible by researchers, lecturers and secretaries in different settings, in episode one, we outlined exactly what type of information the protagonists have access to. To this end, in episode one of the password sharing scenario it was mentioned that the lecturer has access to student information and that the secretary has access to staff information. In the episode one of the email security scenario, the protagonist (the researcher) clearly states that he keeps student information and research data from participants on his laptop. The moral dilemma regarding policy violation was presented in the second episode in which no information about the policy was provided.

Development of the audio records was done with due respect to (1) understandability, (2) realism, (3) absence of unintended moral issues and (4) absence of tip-offs regarding the moral concerns. These were considered according to a list of requirements laid out by Sparks (2015) for a scenario to be effective in researching moral sensitivity. In order to evaluate whether the developed audio records satisfied the aforementioned requirements, we played back the records to four lecturers and researchers familiar with the topic and asked each to determine whether the records satisfied the requirements or not. All evaluators considered the records easily understandable and they all confirmed the absence of unintended moral issues or tip-offs. Regarding realism, most evaluators agreed that audio records reflected very realistic scenarios and three even mentioned that they had experienced a similar situation. However, one evaluator was concerned about the realism of the password sharing scenario on the grounds that in the context of some workplaces one would never ask for someone else's password. However, based on the comments we received from other evaluators who had experienced a similar situation, we deemed the password sharing scenario realistic. In fact, later on during the interviews, some interviewees commented that the password sharing scenario had personally occurred to them.

3.2 Data collection

Nine participants in a Finnish university were interviewed. Participants were university lecturers and researchers, study secretaries (N=7) and students (N=2). Our participants represented the roles present in the audio records (lectures, researchers, secretaries, and students). This fits our goal of exploring moral sensitivity in the specific context (a Finnish university), according to which we developed each audio record. After listening to each audio record, each participant was asked to take the role of the protagonist and answer a number of probing questions. These probing questions included: "What would you say are the issues in this situation?", "Who are the parties involved in this situation?", "What would you say could be done in this situation?", "What would you do in this situation?", "Why did you decide to do this?" and "What arguments could be made against your decision?". Participants' responses were recorded for further analysis. Since compliance with information security policy could be a sensitive issue, a number of measures were taken to avoid potential social desirability bias. To this end, demographic data such as age, and gender were not collected. Furthermore, participants were reassured that their responses would be used and stored confidentially. Lastly, participants were told that there were no right or wrong answers.

During data collection, participants were given the chance to listen to the records multiple times and to consult the scripts in written form if they wished. Despite satisfaction with the understandability of the audio records, this measure was taken to make sure the audio records were fully understandable to non-native English speakers, or those with hearing problems. At the end, only one interviewee asked to consult the written script for the email security scenario and two others asked for listening to the password sharing audio record again.

3.3 Analysis

In order to analyze the data from interviews, we used a thematic analysis approach (Braun & Clarke 2006). Thematic analysis is a reliable method for capturing themes (i.e. important patterns related to a phenomenon) within qualitative data (Braun & Clarke, 2006; Vaismoradi, Turunen, & Bondas, 2013). Drawing on moral sensitivity literature, we followed a deductive thematic analysis (Vaismoradi et al. 2013; Braun & Clarke 2006) to determine participants' sensitivity toward the moral issue in each

scenario. First, we developed a set of codes in three themes according to Rest's (1982) conception of moral sensitivity. These themes included (1) parties involved, (2) course of action possible and (3) consequences. Additional codes in each theme were added during the analysis. Analysis of the interview data was done by two authors, independent from each other. First, the authors listened to recorded interviews to familiarize themselves with the data. Then each author coded the data and wrote a short summary of each interview to reflect their interpretation of the situations. After the first round, the authors compared and discussed the results of their analysis and any potential disagreements. The first round of analysis yielded 92% agreement between the coders (inter-coder reliability) for the password sharing and 85.7% for the email security scenario. All disagreements were resolved after discussion and comparison.

4 Results

To start with, interviewees framed the problem in email security scenario primarily as a security hazard. As well as security, interviewees perceived the problem in the password sharing scenario as a matter of accountability. None of the interviewees framed the problem in either of the two scenarios in moral terms such as welfare, rights or harm. In explaining the security hazard, interviewees often relied on general statements such as "[the secretary] could do other things on [lecturer's] computer" or "the supervisor, I suppose, he has access to some drives, [malware] can infect those drives".

4.1 Identification of Parties involved

Our results indicate that most of the interviewees had difficulty recognizing parties involved in the email scenario. In the email security scenario, most of the interviewees failed to recognize students as parties involved and no one identified research participants even though they were explicitly mentioned in episode one. University or the university network, however, was commonly identified as a party involved. Other colleagues, and IT security team were other parties identified albeit rarely (By two interviewees each). This could reflect interviewees' understanding of the problem in general terms but not in detail. Rather than specifically understanding who could be affected, interviewees identified a larger entity, university in this case, to interpret the situation. They did not see who could be harmed but generally understood that the university was involved. Figure 1 indicates how often each party was identified by the participants.

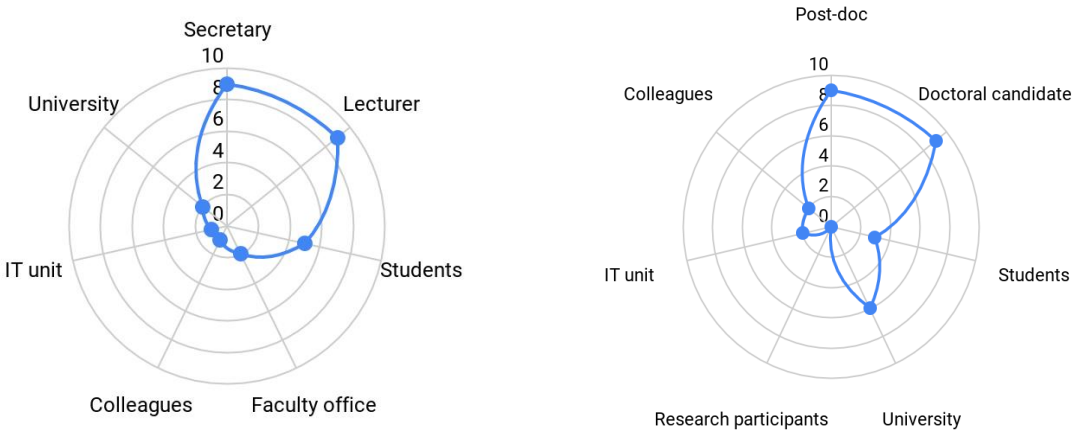

Figure 1. Identification of parties involved (left: password sharing scenario; right: email security scenario).

In the password sharing scenario, other than the lecturer and the secretary, five of the interviewees identified students as a party involved. The faculty office and the university were identified by two while, the IT security team and other colleagues were identified by one interviewee. Recognition of students as a party involved in the dilemma suggests that unlike the email security scenario, in the

password sharing scenario interviewees were sensitive towards security of students' information and by extension students' welfare. However, the finding that the interviewees framed the problem in terms of accountability sheds light on a different aspect of such recognition. Upon hearing the audio records the first reaction of the interviewees was to frame the problem as a matter of security and specifically accountability. Most of the interviewees stated that sharing the password in the scenario meant that the lecturer could be held accountable for something she had no control over. One of the interviewees even went so far to state that sharing the password would be similar to allowing someone to sign off anything on your behalf. Given that the interviewees were asked to take the role of the lecturer, their concern regarding lecturer's accountability suggests that they were first and foremost concerned about protecting themselves in such a situation rather than others.

4.2 Courses of Action

In email security scenario, when asked to outline possible courses of action all interviewees recognized that downloading and opening the attachments was a possibility. Another course of action identified by most interviewees (8 out of 9) was replying to the email either to arrange a meeting, to ask for attachments in a known format or to ask for the content of attachments to be provided in the body of the email. In contrast, only three interviewees suggested asking for help from the IT services.

As for courses of action in password security scenario, some of the interviewees tried to resolve the issue by looking for solutions that was not possible such as a guest account solution or a shared system that should have been implemented before the problem occurred or by negotiating for more time. Others suggested that the lecturer goes to the office in order to submit the grades despite being injured and on a sick leave. These courses of action were suggested as an attempt to avoid sharing the password or violating the deadline. The middle ground course of action that was commonly identified was to deliver the laptop to the lecturer.

4.3 Consequences

When laying down the consequences for downloading and opening the attachments, in the email security scenario, most of the participants sufficed to say that doing so could expose university's information security to threats. Meanwhile, no one noted the risk of exposing research participants' information, and only three interviewees mentioned putting student information in risk. Four interviewees, however, considered the risk of exposing personal information such as recommendation letters. Furthermore, the interviewees failed to see any security problem in replying to the email for any of the parties involved, although two interviewees suspected so. Replying to the email could, however, confirm to a malicious attacker that the email address is indeed active and reveal information regarding the network architecture (e.g. email server and filtering software). Interviewees' failure in understanding the security ramifications of replying to the email indicates lack of security awareness.

For the password security scenario, the interviewees were not able to identify the consequences of the courses of action they had identified on the parties involved. For instance, while all interviewees were aware of the possibility to share the password as a course of action, only four of them were able to realize that sharing the password even temporarily could compromise the security of student information. Moreover, only a few managed to realize that delivering the laptop to the lecturer involves the risk of damaging the laptop or misuse by the delivery person.

5 Discussion and Future Research

Our results suggest that users may not be sensitive towards the moral concerns of security policy compliance. Facing security dilemmas, interviewees did not frame the problem in either of the scenarios in moral terms and explained the dilemmas as security hazards. Furthermore, in the email security scenario interviewees struggled to find the parties involved and in the password scenario they gave more weight to their own protection rather than protection of others' information. This suggests that in security dilemmas users might not be able to identify those who could be harmed by security breaches. This matter could be addressed by highlighting those who could potentially be harmed in the terms of security

policies or as part of the content of security interventions. Additionally, our findings reveal that instructing users in security policies on what is or is not allowed could prove counterproductive. Such an approach could breed a particular interpretation of the security policy not as something to protect information but as a set of rules and regulations that one needs to protect oneself against. In such a case, information security and potential harm to others may become secondary concerns.

Participants' identification of possible courses of action and their consequences seemed flawed. For instance, in the password sharing scenario only four of the participants identified contacting the IT team for solutions such as remote access as a course of action and in the email security scenario only two of the participants identified ignoring the email as a course of action. Meanwhile, in the email security scenario, 8 out of 9 interviewees suggested contacting the applicant by replying to the email without realizing that this course of action could have grave consequences for the welfare of those involved. These findings suggest that lack of security awareness could lead to misinterpretation of moral concerns in security dilemmas. Resultantly, security policies may be inadequate for stimulating users' sense of right or wrong regarding information security and further security interventions may be required.

Without understanding moral concerns in security dilemmas, information system users may not engage in any moral reflection. In such a situation, users' moral beliefs and obligations might become irrelevant to their decisions. Our findings show that this might be the case. While the participants in this study were not completely insensitive toward moral concerns of policy compliance, each one failed in interpreting part of the dilemma; either parties involved, courses of action possible or the consequences of each course of action for the parties involved was ignored by each participants. Therefore, this study raises questions for the common understanding of moral notions and the inhibitory role assigned to them in the literature. Overlooking moral sensitivity could lead to suspect solutions for addressing moral concerns in information security. For instance, a common solution to such concerns in the literature is moral education interventions in which via persuasive arguments users are taught that an action such as security policy violation is morally wrong (Vance & Siponen 2012; Loch & Conger 1996; D'Arcy & Devaraj 2012). Such an intervention, however, may not hit the nail on the head. Instead, it might be necessary to outline those who might be affected by users' security decisions, IT capabilities in an organization and the possible consequences of different courses of action.

In this research in progress, we report the preliminary results of the first step in addressing users' moral sensitivity in information security dilemmas. In next steps, we aim to concentrate on the role of context on users' moral sensitivity by collecting data from other countries and industries in our analysis. As one of our interviewees noted, in some contexts, privacy is valued very highly. This may influence users' moral sensitivity toward information security concerns. Regarding the method, we plan to include a control group in our study in which by using terms such as moral and ethical we provide participants with cues regarding the moral relevance of each security dilemma. This will allow us to empirically verify whether use of such words in the questions changes participants' interpretation of the dilemma. Lastly, based on our findings, we aim to design and conduct a security intervention in which we strive to stimulate moral sensitivity and compare the effectiveness of the method to existing interventions.

Appendix

Password sharing scenario: Ilona is a university lecturer. On her laptop, she has access to student information. Ilona's responsibilities includes grading students. She is required to not share her password with anyone. However, she has recently injured her back and left her laptop at the office. Student grades and information are on her laptop. Markko from the office asks her to either share the password or find another way around the problem.

Email security scenario: Alex is a university lecturer and post-doctoral researcher. On his laptop, he has access to student information and research data from participants. Alex's job requires him to answer emails. However, he is required to watch out for malicious emails and spams. Alex knows that attachments could be harmful. Alex gets an email that looks like it is from a good candidate for doctoral studies. However, the research proposal and the CV are sent in an unfamiliar format to Alex and the email address is a pseudonym.

References

Banerjee, D., Cronan, T.P. & Jones, T.W., 1998. Modeling IT ethics: A study in situational ethics. *MIS Quarterly*, 22(1), pp.31–60.

Bansal, G. et al., 2016. Moral Beliefs and Organizational Information Security Policy Compliance : The Role of Gender. In *MWAIS 2016 Proceedings*.

Bebeau, M.J., Rest, J.R. & Yamoor, C.M., 1985. Measuring dental students' ethical sensitivity. *Journal of Dentail Education*, 49(4), pp.225–235.

Braun, V. & Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), pp.77–101.

Chan, R.Y.K., Ma, K.H.Y. & Wong, Y.H., 2013. The Software Piracy Decision-Making Process of Chinese Computer Users. *The Information Society*, 29(4), pp.203–218.

Cronan, T.P., Leonard, L.N.K. & Kreie, J., 2005. An empirical validation of perceived importance and behavior intention in IT ethics. *Journal of Business Ethics*, 56(3), pp.231–238.

D'Arcy, J. & Devaraj, S., 2012. Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. *Decision Sciences*, 43(6), pp.1091–1124.

D'Arcy, J., Herath, T. & Shoss, M.K., 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, 31(2), pp.285–318.

D'arcy, J. & Hovav, A., 2009. Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics*, 89(SUPPL. 1), pp.59–71.

Dorantes, C.A., Hewitt, B. & Goles, T., 2006. Ethical decision-making in an IT context: The roles of personal moral philosophies and moral intensity. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 8(C), pp.1–10.

Forsyth, D.R., 1980. A taxonomy of ethical ideologies. *Journal of Personality and Social Psychology*, 39(1), pp.175–184.

Goles, T. et al., 2006. Moral Intensity and Ethical Decision-Making: A Contextual Extension. *The DATA BASE for Advances in Information Systems*, 37(2&3), pp.86–95.

Hansen, J. & Walden, E., 2013. The Role of Restrictiveness of Use in Determining Ethical and Legal Awareness of Unauthorized File Sharing. *Journal of the Association for Information Systems*, 14(9), pp.521–549.

Hovav, A. & D'Arcy, J., 2012. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information and Management*, 49(2), pp.99–110.

Hunt, S.D. & Vitell, S., 1986. A General Theory of Marketing Ethics. *Journal of Macromarketing*, 6(1), pp.5–16.

Jones, T.M., 1991. Ethical Decision Making by Individuals in Organizations : An Issue-Contingent Model. *The Academy of Management Review*, 16(2), pp.366–395.

Kim, J. (Jonathan), Park, E.H. (Eunice) & Baskerville, R.L., 2016. A model of emotion and computer abuse. *Information and Management*, 53(1), pp.91–108.

Li, H. et al., 2014. Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, 24(6), pp.479–502.

Li, H., Sarathy, R. & Zhang, J., 2010. Understanding compliance with internet use policy: An integrative model based on command-and- control and self-regulatory approaches. *ICIS 2010 Proceedings - Thirty First International Conference on Information Systems*.

Li, H., Zhang, J. & Sarathy, R., 2010. Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, 48(4), pp.635–645.

Loch, K.D. & Conger, S., 1996. Evaluating ethical decision making and computer use. *Communications of the ACM*, 39(7), pp.74–83.

Moores, T.T. & Chang, J.C.-J., 2006. Ethical Decision Making in Software Piracy: Initial Development and Test of a four-component model. *MIS Quarterly*, 30(1), pp.167–180.

Myyry, L. et al., 2009. What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, 18(2), pp.126–139.

Myyry, L. & Helkama, K., 2002. The Role of Value Priorities and Professional Ethics Training in Moral Sensitivity. *Journal of Moral Education*, 31(1), pp.35–50.

Peterson, D.K., 2002. Computer ethics: The influence of guidelines and universal moral beliefs. *Information Technology & People*, 15(4), pp.346–361.

Rest, J., 1982. A Psychologist Looks at the Teaching of Ethics. *The Hastings Center Report*, 12(1), pp.29–36.

Rest, J., 1986. *Moral development: Advances in research and theory.*, Praeger.

Siponen, M.T. & Vance, A., 2014. Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems*, 23(3), pp.289–305.

Sparks, J.R., 2015. A social cognitive explanation of situational and individual effects on moral sensitivity. *Journal of Applied Social Psychology*, 45, pp.45–54.

Tilahun, A. & Tibebe, T., 2017. Influence Of National Culture On Employees ' Intention To Violate Information Systems Security Policies : A National Culture And Rational Choice Theory. In *25th European Conference on Information Systems (ECIS)*. pp. 2493–2503.

Vaismoradi, M., Turunen, H. & Bondas, T., 2013. Content analysis and thematic analysis : Implications for conducting a qualitative descriptive study. *Nursing and Health Sciences*, 15(3), pp.398–405.

Vance, A. & Siponen, M.T., 2012. IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing*, 24(1), pp.21–41.

Volker, J.M., 1984. *Counseling experience, moral judgement, awareness of consequences and moral sensitivity in counseling practice*. unpublished doctoral dissertation, University of Minnesota, MN.

Yazdanmehr, A. & Wang, J., 2016. Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 92, pp.36–46.

Yoon, C., 2011. Ethical decision-making in the Internet context: Development and test of an initial model based on moral philosophy. *Computers in Human Behavior*, 27(6), pp.2401–2409.